N-14: Portable Devices and Media

Policy: See N-14 Portable Devices and Media at www.cosdcompliance.org

Definitions: See HHSA Policy N-13 Security Definitions

Procedures:

A. Required Authorizations and Tracking

1. No client data shall be removed from any Agency facility, in any format (paper or electronic) without the written approval of the employee's manager or supervisor. This written approval shall be accomplished by the employee and manager or supervisor completing the Safety of Protected Information & Portable Devices Form before the employee removes or transports HHSA Protected Information and completed again if any changes occur to the employee's role involving HHSA Protected Information removal or transport. Once completed, the digitally signed form shall be emailed to Agency Human Resources at Personnel.HHSA@sdcounty.ca.gov for filing in the employee's Agency personnel file. An electronic version of the form is also available at www.cosdcompliance.org .

2. All Agency Executives shall be responsible for maintaining a current inventory of all portable devices and portable media in their program. All acquisition of portable devices and portable media must be County-purchased, have encryption and shall be supported by a business case approved by the appropriate Agency Executive.

3. Program shall report all losses or thefts of client data and/or portable devices or media to the Agency Privacy Officer at PrivacyOfficer.HHSA@sdcounty.ca.gov within 1 business day of discovery of the loss or theft. See **Policy L-24 Privacy Incidents** for further instructions.

B. Security of Data

1. All County owned portable devices (e.g. Laptops, tablet PCs, smartphones) must have hard drive encryption and require a password or PIN to login.
    - Smartphones must be registered in Airwatch MDM

2. No client data shall be downloaded to an employee's personal computer, portable device or portable media at any time.

3. No personal portable device or portable media including, but not limited to, personal MP3 devices/iPods, cell phones, cameras, or personal USB flash/thumb drives, shall be connected to any County electronic device at any time.

Note: Paragraph B.3 does not apply to the personal computers of employees who have received authorization to connect via CITRIX, SSLVPN or other County approved remote access software, nor does it apply to USB flash/thumb drives provided to employees as an attendee at a conference or workshop. Flash or thumb drives provided to conference or workshop attendees who are attending on County time and/or at County expense are considered to be County property.

4. Portable devices or portable media shall not be used for routine storage of client data.

C. Transporting of Data Outside of County Facilities

1. For use during the course of business day. Employees must exercise reasonable precautions to protect client data, as well as portable devices and media.
   a. All client data transported on any portable device or media shall be encrypted.

   b. All client data removed from any County facility, whether in paper or electronic format, must remain in the employee's direct physical possession, or within the employee's direct line of sight, while conducting client visits.

   c. All client data and images contained on any portable media must be downloaded to the employee's County computer (e.g. Desktop, laptop or tablet PC) and erased from the portable media immediately upon the employee's return to their primary work site, if not already downloaded in the field.

   NOTE: Leaving client data, portable devices or media in a vehicle where a passerby can easily see them, is NOT considered reasonable precaution to protect client data.

2. Overnight/Weekend use. Employees must exercise reasonable precautions to protect client data, as well as portable devices and media.

   a. Under no circumstances shall County or Agency owned portable devices, portable media or written or electronic client data be left in a vehicle overnight. All County or Agency owned portable devices, portable media or written or electronic client data kept in an employee's home must be stored in a secure manner.

   b. When traveling on County business, all portable devices and portable media are to be secured in the hotel safe when practical, or kept in the employee's possession. All County or Agency owned portable devices, portable media or written or electronic client data must be kept in the same secure manner as they would if keeping the data in their home.

D. Destruction

Refer to the Mobile Device Disposition Guidelines for all portable devices and media purchased/funded by the County.

E. Lost or Stolen

Refer to Policy L-24 – Privacy Incidents for instructions.

F. Quality Assurance

The Agency Compliance Office shall be responsible for monitoring compliance with this policy.

Violations or suspected violations of this policy will be referred to the Agency Human Resources for appropriate personnel action or investigation.

QUESTIONS/INFORMATION: HHSA Information Security Manager at 619-338-2634